UNITED STATES PATENT AND TRADEMARK OFFICE

UNITED STATES DEPARTMENT OF COMMERCE
United States Patent and Trademark Office
Address: COMMISSIONER FOR PATENTS
P.O. Box 1450
Alexandria, Virginia 22313-1450
www.uspto.gov

APPLICATION NO.	FILING DATE	FIRST NAMED INVENTOR	ATTORNEY DOCKET NO.	CONFIRMATION NO.
09/303,561	05/03/1999	TAKUYA MORISHITA	088941-0129	8535

7590   04/09/2004

FOLEY & LARDNER
WASHINGTON HARBOUR
3000 K STREET NW STE 500
PO BOX 25696
WASHINGTON, DC 200078696

EXAMINER
BAUM, RONALD

ART UNIT	PAPER NUMBER
2136	

DATE MAILED: 04/09/2004

14

Please find below and/or attached an Office communication concerning this application or proceeding.

PTO-90C (Rev. 10/03)

-- The MAILING DATE of this communication appears on the cover sheet with the correspondence address --

Period for Reply

A SHORTENED STATUTORY PERIOD FOR REPLY IS SET TO EXPIRE _3_ MONTH(S) FROM
THE MAILING DATE OF THIS COMMUNICATION.

- Extensions of time may be available under the provisions of 37 CFR 1.136(a). In no event, however, may a reply be timely filed
  after SIX (6) MONTHS from the mailing date of this communication.
- If the period for reply specified above is less than thirty (30) days, a reply within the statutory minimum of thirty (30) days will be considered timely.
- If NO period for reply is specified above, the maximum statutory period will apply and will expire SIX (6) MONTHS from the mailing date of this communication.
- Failure to reply within the set or extended period for reply will, by statute, cause the application to become ABANDONED (35 U.S.C. § 133).
  Any reply received by the Office later than three months after the mailing date of this communication, even if timely filed, may reduce any
  earned patent term adjustment. See 37 CFR 1.704(b).

Status

1) ☒ Responsive to communication(s) filed on _06 February 2004_.

2a) ☒ This action is **FINAL**.   2b) ☐ This action is non-final.

3) ☐ Since this application is in condition for allowance except for formal matters, prosecution as to the merits is
   closed in accordance with the practice under *Ex parte Quayle*, 1935 C.D. 11, 453 O.G. 213.

Disposition of Claims

4) ☒ Claim(s) _1-9_ is/are pending in the application.

   4a) Of the above claim(s) _____ is/are withdrawn from consideration.

5) ☐ Claim(s) _____ is/are allowed.

6) ☒ Claim(s) _1-9_ is/are rejected.

7) ☐ Claim(s) _____ is/are objected to.

8) ☐ Claim(s) _____ are subject to restriction and/or election requirement.

Application Papers

9) ☐ The specification is objected to by the Examiner.

10) ☐ The drawing(s) filed on _____ is/are: a) ☐ accepted or b) ☐ objected to by the Examiner.

   Applicant may not request that any objection to the drawing(s) be held in abeyance. See 37 CFR 1.85(a).

   Replacement drawing sheet(s) including the correction is required if the drawing(s) is objected to. See 37 CFR 1.121(d).

11) ☐ The oath or declaration is objected to by the Examiner. Note the attached Office Action or form PTO-152.

Priority under 35 U.S.C. § 119

12) ☐ Acknowledgment is made of a claim for foreign priority under 35 U.S.C. § 119(a)-(d) or (f).

   a) ☐ All   b) ☐ Some * c) ☐ None of:

   1. ☐ Certified copies of the priority documents have been received.

   2. ☐ Certified copies of the priority documents have been received in Application No. _____.

   3. ☐ Copies of the certified copies of the priority documents have been received in this National Stage
      application from the International Bureau (PCT Rule 17.2(a)).

   * See the attached detailed Office action for a list of the certified copies not received.

Attachment(s)

1) ☒ Notice of References Cited (PTO-892)
2) ☐ Notice of Draftsperson's Patent Drawing Review (PTO-948)
3) ☐ Information Disclosure Statement(s) (PTO-1449 or PTO/SB/08)
   Paper No(s)/Mail Date _____.

4) ☐ Interview Summary (PTO-413)
   Paper No(s)/Mail Date. _____.
5) ☐ Notice of Informal Patent Application (PTO-152)
6) ☐ Other: _____.

DETAILED ACTION

1.   Claims 1- 9 are pending for examination.

2.   Claims 1- 9 remain rejected.

Claim Rejections - 35 USC § 102

The following is a quotation of the appropriate paragraphs of 35 U.S.C. 102 that form the

basis for the rejections under this section made in this Office action:

> A person shall be entitled to a patent unless –
>
> (b) the invention was patented or described in a printed publication in this or a foreign country or in public use or on sale in this country, more than one year prior to the date of application for patent in the United States.

3.   Claims 1-6 are rejected under 35 U.S.C. 102(b) as being anticipated by Atalla, U.S.

Patent 4,588,991.

As per claim 1; "A cryptosystem key updating system for preventing illegal use of

software, comprising [abstract, figure 2,3 and accompanying descriptions]: secret information

storage means for storing secret information [figure 1-3, col. 1,lines 59-col. 2,line 24];

cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret

information stored in the secret information storage means [figure 1-3, col. 1,lines 59-col. 2,line

24]; illegal access determining Means for determining whether an illegal access to the system is

performed [col. 2,lines 7-55, col. 3,lines 50-67]; and cryptosystem key updating means for:

providing the same key for a cryptosystem key used for re-encrypting the secret information

stored in the secret information storage means and a cryptosystem key which is stored as the

updated cryptosystem key in the cryptosystem key storage means if the illegal access

determining means detects no illegal access; providing different keys for the above two kinds of

cryptosystem keys if the illegal access determining means detects an illegal access; and wherein the cryptosystem key updating means updates the above two kinds of cryptosystem keys for each access to the system [figure 1-3, col. 1,lines 59-col. 2,line 55, col. 3,lines 50-67, whereas the sequence of key codes, taken collectively, constitute the applicants cryptosystem key and updated cryptosystem key. Therefore the sequence of new key codes generated in response to an illegal access scenario (i.e., "numerous accesses approaching the limit of key codes ...") corresponds to the applicants different keys limitation.].";

As per claim 2; "A cryptosystem key updating method [This claim is a method claim for the apparatus (system) claim 1 above, and is rejected for the same reasons provided for the claim 1 rejection] for preventing illegal use of software, the method used in a system which comprises a secret information storage means for storing secret information and a cryptosystem key storage means for storing a cryptosystem key used for decrypting the secret information stored in the secret information storage means, the method comprising the steps of: determining whether an access to the system is performed; and for each access to the system, providing the same updated key for a cryptosystem key used for re-encrypting the secret information stored in the secret information storage means and a cryptosystem key which is stored as the updated cryptosystem key in the cryptosystem key storage means if no illegal access is detected in the step of determining whether an illegal access to the system is performed; providing different updated keys for the above two kinds of cryptosystem keys if an illegal access is detected in the step of determining whether an illegal access to the system is performed."

As per claim 3; "A storage medium storing a computer-executable cryptosystem key updating program [This claim is a embodied software claim for the apparatus (system) claim 1

above, and is rejected for the same reasons provided for the claim 1 rejection] for preventing

illegal use of software, the program used in a system which comprises a secret information

storage means for storing secret information and a cryptosystem key storage means for storing a

cryptosystem key used for decrypting the secret information stored in the secret information

storage means, the program including the processes of: determining whether an illegal access to

the system is performed; and for each access to the system, providing the same updated key for a

cryptosystem key used for re-encrypting the secret information stored in the secret information

storage means and a cryptosystem key which is stored as the updated cryptosystem key in the

cryptosystem key storage means if no illegal access is detected in the step of determining

whether an illegal access to the system is performed; providing different updated keys for the

above two kinds of cryptosystem keys if an illegal access is detected in the step of determining

whether an illegal access to the system is performed."

4.   Claim 4 *additionally recites* the limitation that; "A cryptosystem-key updating system for

preventing illegal use of software as claimed in claim 1, wherein the secret information storage

means and the cryptosystem key storage means are separately constructed.". The teachings of

Atalla suggest such limitations (figure 1-3, col. 2,lines 43-col. 3,line 67, col. 5,line 28-col. 6,line

39).

5.   Claim 5 *additionally recites* the limitation that; "A cryptosystem key updating method

[This claim is a method claim for the apparatus (system) claim 4 above, and is rejected for the

same reasons provided for the claim 4 rejection] for preventing illegal use of software as claimed

in claim 2, wherein the secret information storage means and the cryptosystem key storage

means are separately constructed.".

6.   Claim 6 *additionally recites* the limitation that; "A storage medium storing a computer-

executable cryptosystem key updating program [This claim is a embodied software claim for the

apparatus (system) claim 1 above, and is rejected for the same reasons provided for the claim 1

rejection] for preventing illegal use of software as claimed in claim 3, wherein the secret

information storage means and the cryptosystem key storage means are separately constructed.".

Claim Rejections - 35 USC § 103

The following is a quotation of 35 U.S.C. 103(a) which forms the basis for all

obviousness rejections set forth in this Office action:

> (a) A patent may not be obtained though the invention is not identically disclosed or described as set forth in
> section 102 of this title, if the differences between the subject matter sought to be patented and the prior art are
> such that the subject matter as a whole would have been obvious at the time the invention was made to a person
> having ordinary skill in the art to which said subject matter pertains. Patentability shall not be negatived by the
> manner in which the invention was made.

7.   Claims 7- 9 are rejected under 35 U.S.C. 103(a) as being unpatentable over Atalla, U.S.

Patent 4,588,991, and further in view of examiners assertion.

8.   Claim 7 *additionally recites* the limitation that; "A cryptosystem key updating system for

preventing illegal use of software as claimed in claim 1, wherein the system is applied to an IC

card.".

Claim 7 additionally recites the limitation that the system is applied to an IC card. The

examiner takes official notice that an IC card (i.e., smartcard) encompasses the CPU (processing

means), memory (non-volatile, EEPROM), and input/output component that a system such as that recited in the Atalla system would embody (figure 2,3, col. 2,lines 7-23, whereas the typical computer system is modified to include an access securing module, encompassing circuit modules that collectively would be considered a single system element of an IC card).

9.   Claim 8 *additionally recites* the limitation that; "A cryptosystem key updating method [This claim is a method claim for the apparatus (system) claim 7 above, and is rejected for the . same reasons provided for the claim 7 rejection] for preventing illegal use of software as claimed in claim 2, wherein the system in which the method is used is applied to an IC card.".

10.   Claim 9 *additionally recites* the limitation that; "A storage medium storing a computer-executable program [This claim is a embodied software claim for the apparatus (system) claim 7 above, and is rejected for the same reasons provided for the claim 7 rejection] for preventing illegal use of software as claimed in claim 3, wherein the system in which the program is used is applied to an IC card.".

Conclusion

11.   Any inquiry concerning this communication or earlier communications from examiner should be directed to Ronald Baum, whose telephone number is (703) 305-4276. The examiner can normally be reached Monday through Friday from 8:00 AM to 5:30 PM.

If attempts to reach the examiner by telephone are unsuccessful, the examiner's supervisor, Ayaz Sheikh, can be reached at (703) 305-9648. The Fax numbers for the organization where this application is assigned are:

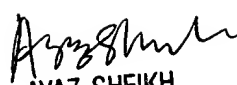After-final   (703) 746-7238

Official   (703) 746-7239

Non-Official/Draft   (703) 746-7246

Ronald Baum

Patent Examiner

AYAZ SHEIKH
SUPERVISORY PATENT EXAMINER
TECHNOLOGY CENTER 2100